UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/508,840	03/08/2005	Christophe Genevois	740612-187	9829

41972 7590 09/16/2008

LAW OFFICES OF STUART J. FRIEDMAN
28930 RIDGE ROAD
MT. AIRY, MD 21771

EXAMINER	
PHAM, LUU T	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/508,840	GENEVOIS, CHRISTOPHE	
	Examiner	Art Unit	
	LUU PHAM	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 June 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *40-65* is/are pending in the application.

4a) Of the above claim(s) *1-39* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *40-65* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is in response to the Amendment filed on 06/17/2008.

2. In the instant Amendment, Claims 1-39 were cancelled. Claims 40-65 have been added; Claim 40 is independent claim. **This action is made FINAL**.

Response to Arguments

3. The objections of claims 6, 14, 21, 23, 25, and 27 are withdrawn as the claims were canceled.

4. The rejections of claims 1-33 and 36-39 under 35 U.S.C. 112, second paragraph are withdrawn as the claims were canceled.

5. The rejections of claims 1-3, 11-13, 15, 20-22, and 24-29 under 35 U.S.C. 101 are withdrawn as the claims were canceled.

6. Applicants' arguments with respect to claims 40-65 have been considered but are moot in view of the new ground(s) of rejection.

Applicants' arguments:

a. Candelore does not teach *"placing the encrypted data packets in the data stream ahead of their original location."* Candelore only teaches *"Preferably, the [encrypted] packets are inserted at the location in the data stream where the single original packet was obtained for encryption* ***so that the sequencing of the data remains essentially the same****."* (emphasis supplied).

The Examiner disagrees for the following reasons:

a. Candelore clearly teaches placing the encrypted data packets in the data stream ahead of their original location *(pars. 0037, 0054-0055, 0064-0068, and 0089; Figs. 3-4 and 7; the encrypted selected packets are passed on to 254 for insertion into the output stream; packet is encrypted as a part of the encryption time slice;* ***the packets making up the encrypted pairs can occur in either order****, but in the preferred implementation, maintain sequence with the clear portion of the PID stream).* (emphasis added). The statement of Candelore in paragraph [0089] ("***Preferably****, the [encrypted] packets are inserted at the location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same.*") is just a description of a "preferred" implementation. Candelore's disclosure still has another option wherein *"the packets making up the* ***encrypted pairs can occur in either order,*** *"* (emphasis added).

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. **Claims 40-41, 45-50, and 54-63 are rejected under 35 U.S.C. 102(e)** as being anticipated by Candelore, U.S. Patent Application No. 2003/0081776, filed on January 02, 2002.

- **Regarding claim 40**, Candelore discloses a conditional access method *(par. 0006; Conditional access (CA) systems are used to control availability of programming in content delivery systems such as cable systems)* wherein digitized multimedia data are transmitted in a continuous transport stream of successive data packets *(pars. 0010, 0046, 0083-0085 and 0089; Figs. 1 and 6-7; digital program streams are broken into packets for transmission; AV content are selected and encrypted and transmitted to cable system 32)*, comprising the steps of, at the generation side:

selectively forming an encrypted transport stream from a base transport stream by detecting particular data packets within the base transport stream *(pars. 0064 and 0089; Figs. 4 and 7; packets are selected at 250 and 350)*, removing and encrypting the particular data packets with an event encryption key *(pars. 0064 and 0089; Figs. 4 and 7; selected packets are passed for encryption to packet encryption process A at step 258 and packet encryption process B at step 262)*, and

inserting the encrypted data packets into the remaining base transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport system *(pars. 0037, 0054-0055, 0064-0068, and 0089; Figs. 3-4 and 7; the encrypted selected packets are passed on to 254 for insertion into the output stream; packet is encrypted as a part of the encryption time slice; the packets making up the encrypted pairs can occur in either order, but in the preferred implementation, maintain sequence with the clear portion of the PID stream; the EA and EB packets are inserted at the*

location in the data stream where the single original packet was obtained for encryption so that the sequencing of the data remains essentially the same).

- **Regarding claim 41**, Candelore discloses the method of claim 40, comprising the step of buffering the non encrypted data packets while the particular data packets are encrypted *(pars. 0064 and 0089; Figs. 4 and 7; steps 254 and 354; the encrypted packets from encryption process A at 258 (EA) are passed on to 254 for insertion into the output stream; the encrypted packets from encryption process B at 262 (EB) are assigned a secondary PID at 264 for insertion into the output stream at 254).*

- **Regarding claim 45**, Candelore discloses the method of claim 40, wherein said encrypted data packets are inserted at positions a predetermined number of data packets ahead of respective original positions *(pars. 0037, 0054-0055, 0064-0068, and 0089; Figs. 3-4 and 7; the encrypted selected packets are passed on to 254 for insertion into the output stream; packet is encrypted as a part of the encryption time slice; the packets making up the encrypted pairs can occur in either order).*

- **Regarding claim 46**, Candelore discloses the method of claim 40, wherein the decryption key is transmitted to a receiver with the selectively encrypted data stream *(par. 0010; additional packets are also included to provide decryption keys and other overhead information).*

- **Regarding claim 47**, Candelore discloses the method of claim 40, wherein the event decryption key is frequently changed *(pars. 0040 and 0082; packets encrypted with*

Motorola's proprietary encryption can use fast changing encryption keys using the embedded security ASIC).

- **Regarding claim 48**, Candelore discloses the system of claim 40, wherein the event decryption key is a fixed key distributed on a pay-per-event basis *(par. 0046; descrambling keys are only distributed to authorized set-top boxes).*

- **Regarding claim 49**, Candelore discloses the system of claim 40, comprising the step of transmitting the event decryption key via a mobile telecommunication network prior to broadcasting the multimedia data *(pars. 0048; the SI (system information) can be separately delivered to both legacy and non-legacy set-top box).*

- **Regarding claim 50**, Candelore discloses the method of claim 40, comprising the step of providing the event decryption key encrypted by a user encryption key, and providing a corresponding user decryption key to an authorized user *(par. 0046; authorized set-top boxes receive Entitlement Control message that are used to get access criteria and descrambling keys).*

- **Regarding claim 54**, Candelore discloses the method of claim 40, wherein the encrypting step comprises the step of producing at a head-end encoder selectively encrypted data stream *(pars. 0046, 0055, 0073, 0083-0085 and 0089; Figs. 1 and 6-7; digital program streams are broken into packets for transmission; AV content are selected and encrypted and transmitted to cable system 32)*, the head-end encoder including an encoder CI module with a Common Interface and Transport Stream CI&TS interface to a professional Set-Top-Box

STB *(Figs. 2-10; cable system head-end 122 transmits data stream to set-top boxes 36 and 136)*.

- **Regarding claim 55**, Candelore discloses the method of claim 40, wherein the base data transport stream is a clear data stream *(pars. 0039, 0056 and 0075; Figs. 4 and 7; substantial portions of content is in clear while encrypting is only a small portions of content)*.

- **Regarding claim 56**, Candelore discloses the method of claim 40, wherein the base transport stream is a DVB-scrambled data stream *(pars. 0005-0006 and 0043; Figs. 1-6; at legacy STB 36, the video is displayed and the encrypted audio is decrypted at CA system A 40 for play on television set 44)*.

- **Regarding claim 57**, Candelore discloses the method of claim 40, wherein all data packets other than the selectively encrypted data packets are DVB-scrambled *(pars. 0045 and 0051; the SI may be scrambled to make it more difficult for a non-authorized set-top boxes)*.

- **Regarding claim 58**, Candelore discloses the method of claim 40, wherein every n^{th} data packet of the transport stream is encrypted, n being a fixed number *(pars. 0056 and 0072-0075; tables 1-2; packets having any of the above four PIDs are again encrypted followed by the next eight time periods being sent in the clear)*.

- **Regarding claim 59**, Candelore discloses the method of claim 40, wherein every nth data packet of the transport stream is encrypted, n being a variable number *(pars. 0072-0075; random value m and n are known as variable numbers)*.

- **Regarding claim 60**, Candelore discloses the method of claim 59, wherein the variable number n is randomly variable *(pars. 0072-0075; pseudo-random and semi-random values for m and n may be used for selection of packets to encrypt)*.

- **Regarding claim 61**, Candelore discloses the method of claim 59, wherein the variable number n is variable as a function of data packet contents *(pars. 0072-0075; pseudo-random and semi-random values for m and n may be used for selection of packets to encrypt)*.

- **Regarding claim 62**, Candelore discloses the method of claim 40, further comprising the steps of, at the reception side *(pars. 0043 and 0065; Figs. 3-8; after distribution through the cable system 32, the video, system information, program specific information, Audio A and Audio B are all delivered to set-top boxes 36 and 136)*:

providing an event decryption key to an authorized receiver having a conditional access system *(par. 0046; authorized set-top boxes receive Entitlement Control Messages (ECM) that are used to get access criteria and descrambling key)*,

transmitting selectively the encrypted transport stream to the receiver *(pars. 0043 and 0065; Figs. 3-8; after distribution through the cable system 32, the video, system information, program specific information, Audio A and Audio B are all delivered to set-top boxes 36 and 136)*,

detecting the encrypted data packets by the conditional access system *(pars. 0065-0069 and 0090; Figs. 5 and 8; when a packet is received at 272, it is inspected to see if it has the primary and secondary PID of interest (step 272 and 274); if the packet has the primary PID of interest, the packet is examined at 284 to determine if the packet is encrypted; if the packet has the secondary PID at 274, the packet is then decrypted at 296 and sent to the packet decoder at 288)*,

removing the encrypted data packets from the received transport stream *(pars. 0065-0069 and 0090; Figs. 5 and 8; the packet is examined at 284 to determine if the packet is encrypted; if the packet has the secondary PID at 274, the packet is then decrypted at 296 and sent to the packet decoder at 288)*,

decrypting the encrypted data packets with the event decryption key *(pars. 0065-0069 and 0090; Figs. 5 and 8; the packet is then decrypted at 296 and sent to the packet decoder at 288)*, and

inserting the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the base transport stream *(pars. 0063-0067 and 0090; Figs. 5 and 8; packets encrypted under CA system B with the secondary PID are decrypted by CA system B 240 and inserted into the clear data stream for decoding and display on television set 244)*.

- **Regarding claim 63**, Candelore discloses the method of claim 62, comprising the step of storing by the conditional access system into a buffer memory, clear data packets while decrypting an encrypted data packet *(pars. 0144-0145; Figs. 17-18; buffers 1006, 1014, 1024, and 1032)*.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

11. **Claims 42-44 and 64-65 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Candelore, as applied to claim 40 above, and further in view of Maillard et al., (hereinafter "Maillard"), U.S. Patent No. US 6,714,650, filed on February 12, 1999.

- **Regarding claim 42**, Candelore discloses the method of claim 40.

Candelore does not explicitly disclose the event decryption key is provided on a one-event smart card.

However, in an analogous art Maillard discloses a method for transmitting and recording digital data wherein the event decryption key is provided on a one-event smart card *(col. 5, lines 54-60; col. 6, lines 4-23; the exploitation key is stored on a smart card)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Maillard with the method and system of Candelore wherein the event decryption key is provided on a one-event smart card to provide users with a means for transmitting and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 43**, Candelore discloses the method of claim 40.

Candelore does not explicitly disclose the event decryption key is provided on a one-limited-period smart card.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the event decryption key is provided on a one-limited-period smart card *(col. 3, lines 22-25; col. 6, lines 4-23; the exploitation key is stored on a smart card)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Maillard with the method and system of Candelore wherein the event decryption key is provided on a one-limited-period smart card to provide users with a means for transmitting and recording of data permitting

authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 44**, Candelore discloses the method of claim 40.

Candelore does not explicitly disclose transmitting the event decryption key in a Digital Video Broadcast DVB environment in specific Entitlement Management Messages EMMs protected by a user encryption key, the corresponding user decryption key being provided in the Control Access System CAS, on a user smart card or on a user Subscriber Identification Module SIM.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data, wherein transmitting the event decryption key in a Digital Video Broadcast DVB environment in specific Entitlement Management Messages EMMs protected by a user encryption key *(col. 2, lines 53-65; the first key is encrypted by a second key)*, the corresponding user decryption key being provided in the Control Access System CAS, on a user smart card or on a user Subscriber Identification Module SIM *(col. 2, lines 19-24; col. 6, lines 4-12; key stored on a smart card is used to decrypt the encrypted ECM and control word)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Maillard with the method and system of Candelore wherein transmitting the event decryption key in a Digital Video Broadcast DVB environment in specific Entitlement Management Messages EMMs protected by a user encryption key, the corresponding user decryption key being provided in

the Control Access System CAS, on a user smart card or on a user Subscriber Identification Module SIM to provide users with a means for transmitting and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 64**, Candelore discloses the method of claim 62.

Candelore does not explicitly disclose conditional access system includes a chip card with decryption circuitry thereon.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein conditional access system includes a chip card with decryption circuitry thereon *(col. 7, lines 44-52; single chip contains descrambling circuitry)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Maillard with the method and system of Candelore wherein conditional access system includes a chip card with decryption circuitry thereon to provide users with a means for transmitting and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

- **Regarding claim 65**, Candelore discloses the method of claim 64.

Candelore does not explicitly disclose the chip card is a SIM card.

However, in an analogous art, Maillard discloses a method for transmitting and recording digital data wherein the chip card is a SIM card *(col. 7, lines 44-52; this chip may be embodied in a SIM card)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method and system of Maillard with that of Candelore wherein the chip card is a SIM card to provide users with a means for transmission and recording of data permitting authorized recording of transmitted digital data, whilst minimizing the risk of pirate copies of such recordings being made by unauthorized third parties *(col. 1, lines 62-67)*.

12. **Claims 51-53 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Candelore, as applied to claim 40 above, and further in view of Thompson et al., (hereinafter "Thompson"), U.S. Patent No. 6,357,046, issued on March 12, 2002.

- **Regarding claim 51**, Candelore discloses the method of claim 40, wherein the encrypting step comprises the step of producing at a head-end encoder the selectively encrypted data stream *(pars. 0042-0044 and 0058; Figs. 2-3; head-ends 122 and 222)*.

Candelore does not explicitly disclose the head-end encoder including a Common Interface CI that in turn has a smart card SC interface for a smart card that has encryption circuitry thereon.

However, in an analogous art, Thompson discloses a method for continually updating and retrieving interactive video information, wherein the head-end encoder including a Common Interface CI that in turn has a smart card SC interface for a smart card

that has encryption circuitry thereon *(col. 7, lines 14-24; Fig. 6; smart card 11, smart card interfaces 15, and head-end computer 16).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Thompson with the method and system of Candelore wherein the head-end encoder including a Common Interface CI that in turn has a smart card SC interface for a smart card that has encryption circuitry thereon to provide an interactive, video display, data system that affords security to the cable company or other distributor against unauthorized access to the database *(col. 2, lines 25-29).*

- **Regarding claim 52**, Candelore discloses the method of claim 40, wherein the encrypting step comprises the step of producing at a head-end encoder the selectively encrypted data stream *(pars. 0042-0044 and 0058; Figs. 2-3; head-ends 122 and 222).*

Candelore does not explicitly disclose the head-end encoder including a Common Interface CI for a Personal Computer PC card module that has encryption circuitry thereon.

However, in an analogous art, Thompson discloses a method for continually updating and retrieving interactive video information, wherein the head-end encoder including a Common Interface CI for a Personal Computer PC card module that has encryption circuitry thereon *(col. 7, lines 14-24 and 39-58; Fig. 6; head-end computer 16, smart card interfaces 15, and smart card 11).*

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Thompson with the method and system of Candelore wherein head-end encoder including a Common Interface CI for a

Personal Computer PC card module that has encryption circuitry thereon to provide an interactive, video display, data system that affords security to the cable company or other distributor against unauthorized access to the database *(col. 2, lines 25-29)*.

- **Regarding claim 53**, Candelore discloses the method of claim 40, wherein the encrypting step comprises the step of producing at a head-end encoder selectively encrypted data stream *(pars. 0042-0044 and 0058; Figs. 2-3; head-ends 122 and 222)*.

Candelore does not explicitly disclose the head-end encoder including a PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC.

However, in an analogous art, Thompson discloses a method for continually updating and retrieving interactive video information, wherein the head-end encoder including a Common Interface CI for a Personal Computer PC card module that has encryption circuitry thereon *(col. 7, lines 14-24 and 39-58; Fig. 6; head-end computer 16)*.

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teaching of Thompson with the method and system of Candelore wherein the head-end encoder including a PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC to provide an interactive, video display, data system that affords security to the cable company or other distributor against unauthorized access to the database *(col. 2, lines 25-29)*.

Conclusion

13. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luu Pham whose telephone number is 571-270-5002. The examiner can normally be reached on Monday through Friday, 7:30 AM - 5:00 PM (EST).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information

for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luu Pham/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137